(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 April 2004 (22.04.2004)

PCT

(10) International Publication Number
WO 2004/034229 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/032268

(22) International Filing Date: 10 October 2003 (10.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/417,674 10 October 2002 (10.10.2002) US

(71) Applicant *(for all designated States except US)*: **ROCKSTEADY NETWORKS, INC.** [US/US]; 3410 Far West Blvd., Suite 210, Austin, TX 78731 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MACKINNON, Richard** [US/US]; 4201 Speedway, Austin, TX 78751 (US). **LOONEY, Kelly** [US/US]; 10737 Chestnut Ridge, Austin, TX 78726 (US). **WHITE, Eric** [US/US]; 1717 Bartoncliff Drive, Austin, TX 78704 (US).

(74) Agent: **ADAIR, John, L.**; Gray Cary Ware & Freidenrich, LLP, 1221 South MoPac Expressway, Suite 400, Austin, TX 78746 (US).

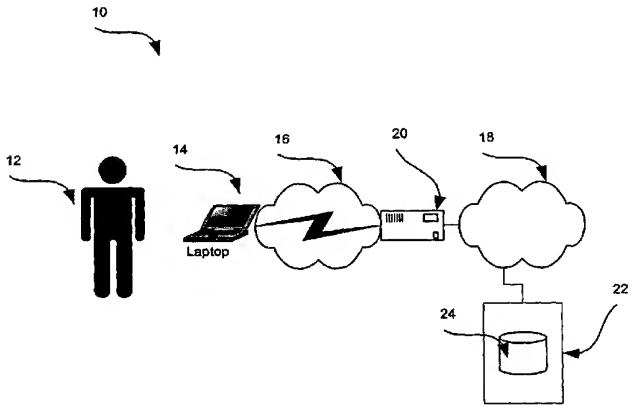
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL



(57) Abstract: More particularly, one embodiment of the present invention provides a system of providing network access comprising a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media, executable by the processor. In one embodiment of the present invention, the computer instructions can be executable to receive a network communication over the first network interface from a user using a user device and determine if the network communication is associated with an authenticated user. If the network communication is not associated with an authenticated user, the computer instructions can be executable to direct the user to an authentication interface. The computer instructions can be further executable to receive credentials from the user and authenticate the user based on the credentials. Another embodiment of the present invention can include a system for providing access to a network that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media. The computer instructions can be executable by the processor to receive a user profile and provision a user with access to a network based on the user profile.

WO 2004/034229 A2

DESCRIPTION

SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL

TECHNICAL FIELD

Embodiments of the present invention relate to network access. More particularly, embodiments of the present invention relate to providing access control for a shared network.

BACKGROUND

The communication of data over networks has become an important, if not essential, way for many organizations and individuals to communicate. The Internet is a global network connecting millions of computers using a client-server architecture in which any computer connected to the Internet can potentially receive data from and send data to any other computer connected to the Internet. The Internet provides a variety methods in which to communicate data, one of the most ubiquitous of which is the World Wide Web. Other methods for communicating data over the Internet include e-mail, usenet newsgroups, telnet and FTP.

Users typically access the Internet either through a computer connected to an Internet Service Provider ("ISP") or computer connected to a local area network ("LAN") provided by an organization, which is in turn, connected to the ISP. The ISP provides a point of presence to interface with the Internet backbone. Routers and switches in the backbone direct data traffic between the various ISPs.

To access a LAN and, in turn, the Internet, many prior art access control systems require a user to connect his or her computer to a wired network (e.g., through an Ethernet port) and enter a user name and password. If the user name and password match a user name and password in an authentication database, the user will be provided access to the network. These systems typically assume that a user is tied to a particular physical port, such as a port in the user's office. Based on this assumption, provisioning of bandwidth to the user occurs by physically provisioning the port to which the user is connected. If the user moves to a different port, the user will typically be provided with the bandwidth provisioned to the new port. Thus, provisioning of bandwidth is done on a per port rather than a per user basis.

General internet access provided via broadband technology (e.g., Digital Subscriber Line, DOCSIS or analog cable modem, or similar technologies) are capable of provisioning bandwidth to a computer premise equipment (CPE) device. CPE provisioning can be dynamic and remotely administered. However, broadband technology adoption is not a single-user and, hence, is not user-specific provisioning.

An increasing number of organizations (e.g., businesses, governmental organizations) wish to provide access to LANs and the Internet to various classes of users (internal users, contractors, customers, visitors). For example, many cafés have public wireless networks to allow patrons to access the Internet, receive email and perform other network activities. While users may be asked to authenticate to use the network, bandwidth is provisioned to the wireless routers, not the individual users. This means that one user connected to a particular router can consume a majority of the bandwidth (e.g., downloading pictures from the Internet), slowing down the wireless network for other users connected to that router.

An additional problem with many current networks, particularly wireless networks, is roaming between subnets. A subnet is a portion of a LAN that has a common address component. One subnet, for example, can cover a particular floor of a building, while another subnet covers another floor. Each subnet can potentially have its own set of internet protocol ("IP") addresses that may or may not overlap with the IP addresses of other subnets. When a user moves from one subnet to another, even if both subnets are part of the same LAN, the user must typically reauthenticate with the network. This can make physically roaming between subnets frustrating because open network sessions will often be dropped.

DISCLOSURE OF THE INVENTION

Embodiments of the present invention provide a system and method of providing network access that eliminates, or at least substantially reduces, the shortcomings of prior art network access systems and methods. More particularly, one embodiment of the present invention provides a system of providing network access comprising a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media, executable by the processor. In one embodiment of the present invention, the computer instructions can be executable to receive a network communication over the first network interface from a user using a user device and determine if the network

communication is associated with an authenticated user. If the network communication is not associated with an authenticated user, the computer instructions can be executable to direct the user to an authentication interface. The computer instructions can be further executable to receive credentials from the user and authenticate the user based on the credentials. If the user is authenticated, the computer instructions can receive a user profile.

Another embodiment of the present invention can include a system for providing access to a network that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media. The computer instructions can be executable by the processor to receive a user profile and provision a user with access to a network based on the user profile.

Another embodiment of the present invention includes a set of computer instructions stored on a storage media, executable by a processor to receive a network communication over a first network interface from a user using a user device, determine if the network communication is associated with an authenticated user, if the network communication is not associated with an authenticated user, direct the user to an authentication interface, receive credentials from the user, authenticate the user based on the credentials. If the user is authenticated, the computer instructions can be executed to receive a user profile.

Yet another embodiment of the present invention includes a set of computer instructions stored on the storage media, executable by the processor to receive a user profile and provision a user with access to a network based on the user profile.

Another embodiment of the present invention includes a method comprising receiving a user profile and provisioning a user with access to a network based on the user profile.

Another embodiment of the present invention includes a method comprising receiving a network communication over a first network interface from a user using a user device, determining if the network communication is associated with an authenticated user, if the network communication is not associated with an authenticated user, directing the user to an authentication interface, receiving credentials from the user, authenticating the user based on the credentials, and receiving a user profile if the user is authenticated.

Embodiments of the present invention provide an advantage over current systems and methods of providing access to a network by being able to authenticate a user sending network communications in any number of protocols.

Embodiments of the present invention provide another advantage over current systems and methods of providing access to a network by not requiring propriety client software to authenticate.

Embodiments of the present invention provide yet another advantage over current systems and methods of providing network access by provisioning network access on a per user rather than per port basis.

Embodiments of the present invention provide yet another advantage over current systems and methods of providing network access by supporting the ability of a user to physically roam without requiring reauthentication on different subnets.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention and the advantages thereof may be acquired by referring to the following description, taken in conjunction with the accompanying drawings in which like reference numbers indicate like features and wherein:

FIGURE 1 is a diagrammatic representation of a system for providing network access according to one embodiment of the present invention;

FIGURE 2 is a flow chart illustrating one embodiment of a method for providing network access control;

FIGURE 3 is a flow chart illustrating one embodiment of provisioning user access to a network;

FIGURE 4 is a diagrammatic representation of a software architecture for providing authentication, according to one embodiment of the present invention;

FIGURE 5 is a diagrammatic representation of one embodiment of a software system for controlling access to a network for an authenticated user;

FIGURE 6 is a diagrammatic representation of traffic conditioning module, according to one embodiment of the present invention;

FIGURE 7 is a diagrammatic representation of roaming according to one embodiment of the present invention; and

FIGURE 8 is a diagrammatic representation of an example embodiment of a control device.

DETAILED DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention are illustrated in the FIGURES, like numerals being used to refer to like and corresponding parts of the various drawings.

Embodiments of the present invention provide a system and method of network access control. According to one embodiment of the present invention, a control device can sit between a network (e.g., an Internet, a LAN or other network known in the art) and users. The users themselves may be located on a network or subnet or may connect directly to the control device. When a particular user attempts to access the network behind the control device (i.e., the controlled network), the control device can determine if the user has already been authenticated to use the controlled network. If the user has not been authenticated, the control device can direct the user to an authentication interface, such as a web page, and receive a set of credentials from the user. If the user is authorized to use the controlled network, based on the credentials, the control device can provision the user with access to the controlled network based on user specific settings.

FIGURE 1 is a diagrammatic representation of a system 10 for providing network access according to one embodiment of the present invention. In system 10, a user 12, using a user device 14 on network 16, can send a network communication that is destined for a device on controlled network 18. Network 16 and controlled network 18 can be any networks known in the art including, but not limited to, LANs, WANs, the Internet, global communications networks, wireless networks and/or any other communications network known in the art. For the sake of example, network 16 can be a wireless network, such as public wireless network provided to café patrons, and controlled network 18 can be the Internet. An access control device 20 ("control device 20") can receive the network communication and determine if user 12 is authorized to access network 18 and the extent of the user's access. Control device

20 can contact an authentication system 22 to authenticate user 12 against a set of authorized users stored, for example, in authentication database 24. If user 12 is authenticated, access control device 20 can receive a user profile that includes one or more attributes that govern the user's access to controlled network 18.

According to one embodiment of the present invention, user device 14 can comprise any computing device known in the art (e.g., desktop, laptop, PDA, mobile phone or any other device capable of network communication) and can be connected to control device 20 in any manner known in the art (e.g., by LAN, wireless network, direct connection or other manner known in the art). In the example of FIGURE 1, user 12 is using a laptop 14 on a public wireless network 16 (e.g., a wireless LAN) to access Internet 18.

User 12 can send the network communication using a network application running on user device 14 destined for a device on network 18. The network application can be any publicly available network application (e.g., a web browser, email program, etc.) or proprietary application. For example, user 12 can use an internet browser, such as Netscape Navigator or Microsoft Internet Explorer, to send a request for a web page available over Internet 18. As would be understood by those of ordinary skill in the art, the web page request is transmitted as an HTTP request in one or more internet protocol ("IP") packets.

Control device 20 can monitor network 16 for network communications originating on network 16 (e.g., for example for IP packets originating on LAN 16) using any network monitoring technique known in the art. Control device 20 can read the IP packet headers to extract information on the originating user device. As an example, control device 20 can read the packet headers corresponding to the web page request to determine the IP address and MAC address associated with laptop 14.

Based on the MAC address, IP address or other information that can be extracted from the network communication, control device 20 can determine if user 12 has been authenticated. This can be done, for example, by comparing the MAC address and IP address of user device 14 to MAC addresses and IP addresses for users that have been authenticated. If the user has not authenticated, control device 20 can direct user 12 to an authentication interface by, for example, redirecting the HTTP request to a login web page that requests user credentials, such as user name and password.

Control device 20 can receive the user credentials and send the credentials to authentication system 22. Authentication system 22 can compare the credentials to credentials in authentication database 24 to determine if user 12 is permitted access to network 18 and the extent of the user's access. If the credentials are authenticated, authentication system 22 can pass a user profile associated with user 12 to control device 20.

The user profile can include parameters that determine the extent of a user's access to network 18 and/or services available to that user. For example, the user profile can indicate that a user is permitted certain upload and download data transfer rates, that the user is not permitted to visit particular web sites, or that the user qualifies for virus scanning. In one embodiment of the present invention, the constraints indicated in the user profile can be implemented through one or more applications at control device 20.

When control device 20 receives a user profile from authentication system 22 (or self authenticates the user), control device 20 can establish a control session for the user, indicating that the user is currently active. Additionally, control device 20 can establish provisioning rules based on the user profile. The provisioning rules can include, for example, firewall rules and traffic constraints that govern the user's access to network 18. In one embodiment of the present invention, the sessions and provisioning rules can be indexed to a particular user. This can be done, for example, by associating the control session and rules to a key based on the MAC address and/or IP address of laptop and/or user credentials. The use of user credentials as part of an indexing key allows multiple sessions by the same user using different devices (e.g., a user accessing network 18 through a laptop and PDA) to be tied together for, for example, billing purposes.

It should be noted that FIGURE 1 is provided by way of example only. In other embodiments of the present invention, control device 20 can control access to multiple networks. For example, if a user requests a web page over a cafés publicly available wireless connection, the user may need to access both additional portions of the café's internal LAN (e.g., routers, switches or other network devices) and the Internet. Additionally, it should be noted that authentication, in one embodiment of the present invention, can be performed at control device 20 or be carried out by a separate authentication system.

FIGURE 2 is a flow chart illustrating one embodiment of a method for providing network access control at, for example, a control device (e.g., control device 20 of FIGURE 1). At

step 30, the control device can monitor a connection, such as a LAN, across protocol layers (e.g., IP, UPD/IP, TCP/IP and other protocol layers known in the art) for a network communication originating at a user device and, at step 32, receive a network communication. The network communication can be, for example, an HTTP request, an email message, an FTP request, a telnet request, an instant message, an ICMP message, a SNMP message, a UDP message or other network communication known in the art.

The control device can determine, at step 34, if a user associated with the network communication has been authenticated. In one embodiment of the present invention, this can be done by comparing an identifier(s) with identifiers previously associated with authenticated users. Any identifier or combination of identifiers known in the art can be used to identify the origins of a network communication. By way of example, but not limitation, the control device can read the headers of IP packets carrying the network communication to extract an originating MAC address and/or an originating IP address associated with the originating user device. The control device can compare the identifier(s) extracted from the IP packet to identifiers for previously authenticated users. If the extracted identifier matches an authenticated user, the control device can control the user's network access as described in conjunction with the example of FIGURE 5. Otherwise, control can pass to step 36.

If a user has not authenticated, the control device, at step 36, can capture the user's network application session until the user authenticates. For applications that are latency or session sensitive, such as HTTP or HTTPS communications, the session may be cached or suspended in a manner that does cause the destination application (e.g., web page) to drop the session. For example, if the user enters into a stateful network application session, the control device can detect this, based on information in the IP packets, and maintain the session on behalf of the user until the user has authenticated.

At step 38, the control device can redirect the user to an authentication interface. By way of example but not limitation, if the network communication is an HTTP request, control device 20 can redirect the HTTP request to an authentication web page hosted by the control device using any HTTP redirection technique known in the art. If the network communication is in another form, such as an email message, the control device can detect, from the IP packets, the protocol (e.g., POP, SMTP or other protocol known in the art) used by the network application (e.g., a mail user agent) and send a message back to the network

application with, for example, an embedded link to the authentication interface. In other embodiments of the present invention, the control device can send a protocol-specific message, such as an error message, indicating the authentication state and providing information about further actions necessary on part of the user to authenticate. As an example, if an unauthenticated user initiates a telnet session, the control device can return a telnet error indicating a failed authentication and providing directions to the application interface. Thus, the control device, rather than simply returning "Connect Failed" could return "Connect Failed: Authenticate at http://www.Rocksteady1.com/login//." In this case, http://www.Rocksteady1.com/login// can be hosted by the control device.

In response to the authentication interface, the user can provide credentials and, at step 40, the control device can receive them. The credentials can be any credentials known in the art including, but not limited to, user name, password, biometric data (e.g., fingerprint, retina pattern or other biometric information known in the art), smart card credentials, certificates and/or other user or hardware based credentials. In one embodiment of the present invention, the credentials can be received by HTTP Post from a web page based form.

At step 42, the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users. This can be done at the control device, or the control device can authenticate the user by sending the credentials to a backend authentication system (e.g., using HTTP Post). The credentials, in one embodiment of the present invention, can be compared against an authentication database of authorized users to determine if the credentials match credentials in the authentication database. Example authentication technologies include LDAP, RADIUS, Microsoft Active Directory Service, Tivoli Access Manager, and Cisco TACACS/TACACS+.

If the credentials are not authenticated, control can pass to step 52. If, on the other hand, the credentials are authenticated, the control device, at step 44, can receive a user profile from the authentication system or internal data storage (e.g., a database, file or other data storage format known in the art) that contains attributes that govern provisioning of user access to the network. For example, the user profile can contain indicators of the upload and download bandwidth to which the user is entitled, session time limit, whether the control device will perform virus scanning for the user of incoming and/or outgoing IP packets, or other services known in the art. The user profile can also point to additional information that can be used to

control network access. For example, the user profile can point to a list of web sites that the particular user is not permitted to visit. In one embodiment of the present invention, the user profile can be received in a canonical format as an HTTP Post from the authentication system to the control device.

According to one embodiment of the present invention, each user profile can have a predefined set of attributes. In some cases, the backend authentication system may not provide values for each of these attributes. Therefore, the control device can determine, at step 46, if the received user profile is complete, and, if it is not complete can, at step 48, fill in the missing attribute values with default values, which can be part of the control device's local configuration or may be retrieved by the control device during, for example, its initialization or startup phase. At step 50, the control device can initiate a control session for the authenticated user. The control session can have a specified time limit, a time out limit and/or other session features known in the art. While the control session is active, the control device can govern a user's access to a network according to the user profile associated with that user and defaults. The control session can be tracked by credentials, IP address, MAC address and/or other identifier. In one embodiment of the present invention, the control session can be tracked based on a combination of user device MAC address and IP address and user provided credentials.

Thus, the control device can determine if the user seeking to use a network is authorized to use the network (step 42). According to one embodiment of the present invention, if the user is authenticated, the control device receives a user profile (step 44), fills in any missing parameters in the user profile with defaults (steps 46 and 48) and initiates a control session for the user (step 50).

If, however, at step 42, the user is not authenticated, the control device, at step 52, can direct the user to a setup interface, such as an account setup web page. At the setup interface, the user can specify credentials, network access and levels of service, payment options and/or other account information. Based on this information, a user profile can be generated and stored in the authentication database. Profiles can also be entered into the authentication database by a systems administrator or in any other manner known in the art.

The control device can, thus, authenticate a user based on a network communication from a network application such as a web browser, ftp client, telnet client, mail user agent or other

publicly available or proprietary network application. By supporting publicly available network applications, such as web browsers, embodiments of the present invention allow authentication without requiring that a user install a proprietary network application on the user's user device. If a user can authenticate, the control device can control a user's access to a controlled network based on a user profile and/or default values. If the user can not authenticate, the user can be given an opportunity to establish a user profile. According to one embodiment of the present invention, steps 30-54 can be optionally repeated (step 54) for each new network communication or IP packet detected.

FIGURE 3 is a flow chart illustrating one embodiment of provisioning user access to a network at a control device (e.g., control device 20 of FIGURE 1). At step 56, global rules can be established. Global rules can include rules, such as firewall rules and bandwidth allocations. A firewall rule can include any firewall rule known in the art, such as, for example, that all packets destined for a particular web site will be blocked. A traffic rule can include any globally applicable traffic rule; for example, that the total used bandwidth of control device 20 must not exceed a particular amount. Additionally global rules can include rules such as that every packet is scanned for viruses or subject to some other arbitrarily defined process. At step 58, interface specific rules can be established. Interface specific rules can specify and arbitrary traffic rule or condition on a per interface basis. For example, an interface specific firewall rule can specify that streaming content will not be permitted over a wireless interface. Global and interface specific rules can be established in any manner, as would be understood by those of ordinary skill in the art.

At step 60, the control device can establish user specific rules and conditions based on attributes in the user profile. According to one embodiment of the present invention, the control device can map the attributes to any arbitrary rule or traffic condition. By way of example, but not limitation, a user profile can contain attributes to specify upload and download bandwidth allocations for a user, firewall settings, whether the user can use transient VPNs, whether the user can use streaming services or voice over IP services, whether the user should be permitted to perform video teleconferencing, whether the control device should perform virus scanning or worm detection for the user, whether the user can utilize print services, surcharges for services or other settings.

In one embodiment of the present invention, rules can be represented in an IP table. As would be understood by those of ordinary skill in the art, IP tables are essentially tables of rules that can be accessed by applications, such as a firewall, to execute the rules. Rules in the IP table can be associated to a user through any arbitrary identifier. Using the example of FIGURE 1, the IP table rule(s) for user 12 can be bound to user 12 based on the MAC address and IP address of user device 14 and the credentials provided by user 12 for the particular control session.

An IP table rule can reference other rules or parameters for providing user specific provisioning. As an example, the IP table rule can reference websites that a user is not permitted to visit. A firewall application can access the rule to prevent the user from visiting these sites. As another example, the IP table rule for user 12 can reference a traffic rule that dictates that the bandwidth allocated to user 12 is 128kbps up and 512kbps down. A traffic control application, such as the Linux based Traffic Control module, can access the traffic control rule through the IP table and enforce the bandwidth allocation.

It should be noted that a user specific rule in an IP table can reference rules or parameters usable by any number of applications or process, such as firewalls, traffic control modules, virus scan applications or other applications known in the art. For example, a virus scan application can access the IP table rule for a particular user and us parameters referenced by the rule to provide user specific virus scanning. It should be further noted that the use of IP tables to establish user specific rules for user specific provisioning of bandwidth and access control is provided by way of example only, and user specific rules can be implemented in any suitable manner, as would be understood by those of ordinary skill in the art

FIGURE 4 is a diagrammatic representation of a software architecture for providing authentication, according to one embodiment of the present invention. The software architecture can be implemented, for example, at control device 20. According to one embodiment of the present invention, an authentication module 62 of an authentication and control program 61 can monitor a connection, such a network connection for communications from user devices. Control device 20 can receive a network communication in the form of, for example, one or more IP packets 63, which can represent a network communication from a web browser, a telnet client, a mail user agent or other communication from a network application. In one embodiment of the present invention, the network

communication can be directed to control device 20 to access authentication page 70 or to another destination, such as a web server on the Internet.

Authentication module 62 can read the header 64 of IP packet 63 to determine an identifier for the originating user device such as, for example, an originating MAC address and/or IP address. For the sake of example, the MAC address is 08:00:69:02:01:FF and the IP address is 100.100.100. Authentication module 62 can then determine if the IP packet originated at a user device for which a control session is active by comparing information extracted from the header to a list 66 of active control sessions. The active control sessions can be indexed by, for example, MAC address, IP address, a combination of addresses or other identifier(s) associated with the originating user device or user. If a control session is active for the originating user device, the IP packet and header information can be passed to provisioning module 68. If the IP packet originated at a user device not associated with an active control session, control device 20 can authenticate the user.

According to one embodiment of the present invention, to authenticate the user, control device 20 can redirect the user to an authentication interface, such as authentication web page 70, by sending a redirect message 72. Redirect message 72 can be a web page redirect, an error message, an email message with an embedded link to web page 70 or other indication that a user should access the authentication interface.

A user can provide credentials 74 to control device 20 and control device 20 can pass the credentials 74 to an authentication system as, for example, an HTTP Post. If the credentials are authenticated by the authentication system, authentication module 62 can receive a user profile 76 that contains attributes that can govern provisioning of access control for the user. In one embodiment of the present invention, if the user profile is incomplete, authentication module 62 can add default attributes to the profile. Furthermore, if the user is authenticated by the authentication system, session monitor 78 can initiate a new control session if the credentials are authenticated and update the list 66 of active control sessions. It should be noted that in another embodiment of the present invention, authentication can occur internally to control device 20.

FIGURE 5 is a diagrammatic representation of one embodiment of a software system for controlling access to a network for an authenticated user. According to one embodiment of the present invention, an authentication and control program 61 running at control device 20

can receive an IP packet 80 originating from a user device. Authentication module 62 can determine if IP packet 80 is associated with a user that has authenticated, as described in conjunction with FIGURE 4. Continuing with the previous example, and assuming that the user associated with MAC address 08:00:69:02:01:FF and the IP address 100.100.100 authenticated, IP packet 80 can be processed by provisioning module 68, which can provide user specific provisioning. In the example of FIGURE 5, user specific provisioning can include provisioning of firewall services (e.g., by firewall module 82), user specific allocation of bandwidth (e.g., by traffic conditioning module 84). It should be understood, however, that user specific provisioning can include provisioning of additional services known in the art. In one embodiment of the present invention firewall module 82 can be a LINUX based firewall and traffic conditioning module 84 can be the LINUX based Traffic Controller program.

According to one embodiment of the present invention, provisioning module 68 can build a set of IP tables to govern provisioning by firewall module 82 and traffic conditioning module 84. In the example of FIGURE 5, provisioning module 68 can have IP table 86 for interface specific rules, IP table 88 for global rules and IP table 90 for user specific rules. IP table 90 can contain user specific rules associated with particular users. For example, IP table 90 can contain user rule 92 indexed to MAC address 08:00:69:02:01:FF and the IP address 100.100.100 (i.e., indexed to user 12 on laptop 14).

Each rule can optionally point to additional rules and parameters. For example user specific rule 92 can point to traffic control rule 94 to govern bandwidth provisioning, firewall parameters 96 to govern firewall settings and file 98 that contains web sites that user 12 is not permitted to access. User specific rule 92 and the associated rules and parameters can be based on user profile 76. As an example, user profile 76 can specify that user 12 is entitled to 128kbps up and 512kbps down. Provisioning module 68 can establish traffic control rule 94, accessible by traffic conditioning module 84, that contains these limitations. Similarly, provisioning module 68 can establish firewall parameters 96 and file 98 based on attributes in user profile 76.

In the example of FIGURE 5, provisioning module 68 can provide firewall and traffic conditioning services for IP packet 80. Firewall module 82, in one embodiment of the present invention, can process IP packet 80 according to several stages. At interface specific

stage 98, firewall module 82 can access interface specific IP table 86 to access rules to be applied to packet 80 based on the type of interface over which packet 80 is received (e.g., wireless, Ethernet, or other interface known in the art). At global stage 100, firewall module 82 can apply global firewall rules to packet 80 from global IP table 88. In general, firewall module 82 can apply global firewall rules to every IP packet that firewall module 82 processes.

At client discrimination stage 102, firewall module 82 can read the packet header of packet 80 to extract information to associate packet 80 with a user. Continuing with the previous example, if firewall module 82 extracts MAC address 08:00:69:02:01:FF and the IP address 100.100.100, firewall module 82 can associate packet 80 with user specific rule 92. At user specific rule stage 104, firewall module 82 can access user specific rule 92 based, for example, on the extracted MAC address and IP address. Based on user specific rule 92, firewall module 82 can access firewall parameters 94 and restricted web site list 96 and can process packet 80 accordingly. It should be noted that firewall parameters 94 can include any arbitrary set of parameters that can be used by a firewall to control traffic flow. For example, firewall parameters 94 can specify whether the associated user (e.g., user 12 of FIGURE 1) can use voice over IP applications, video conferencing services, transient VPN applications or other applications. Finally, at interface specific stage 106, firewall module 82 can access interface specific IP table 86 and enforce rules corresponding to the interface over which packet 80 will be communicated (e.g., wireless connection, Ethernet connection, or other computer interface known in the art).

In one embodiment of the present invention, traffic conditioning module 84 can also access user specific IP table 90 and locate user specific rule 92, based for example, on the originating MAC address and IP address. From user specific rule 92, traffic conditioning module 84 can locate traffic control rule 94 that specifies a maximum upload bandwidth of 128kbps. If the user exceeds this bandwidth limitation, traffic conditioning module 84 can queue or drop packet 80.

Packet flow in the reverse direction can be processed in an analogous manner. For example, a packet arriving from the Internet destined for a user device (e.g., laptop 14 of FIGURE 1) can be examined for IP address and MAC address. Based on these identifiers, user specific traffic control rules and firewall rules can be applied to the packet as governed by user

specific rule 92 in IP table 90. Firewall module 82 can apply global rules based on IP table 88 and interface specific rules based on IP table 86 for both the controlled network and user side interfaces.

In addition to authentication and provisioning, authentication and control program 61 can provide session monitoring. Session monitoring can be performed in any manner known in the art. Session monitor 78 can monitor a control session for session characteristics such as session time, time out, bandwidth utilization and other session characteristics known in the art. In one embodiment of the present invention, session monitor 78 can determine if a user's session is still active by for example, performing port scans and ARP pings, as would be understood by those of skill in the art. If session monitor 78 determines that a control session is timed out (e.g., has been inactive for a predetermined period of time), session monitor can remove the control session from the list of active sessions, returning the user to an unauthenticated state, and delete the user specific rules for the associated user from IP table 90. Session monitor 78 can also generate records, such as accounting records and session records that can optionally be transmitted to other systems for further processing.

As would understood by those of ordinary skill in the art, authentication and control program 61 can also provide any arbitrary services known in the art, including, but not limited to, web server functions, DHCP client for negotiation with ISPs, DHCP server to assign IP addresses to user computers, kernel based packet filtering and stateful inspection, IP sharing, NATplus, port redirection, information and attack logging, automatic updating, VPN masquerade, remote support an configuration, name server configuration and/or web content filtering.

FIGURE 6 is a diagrammatic representation of traffic conditioning module 84, according to one embodiment of the present invention. Conditioning module 84 can include interface master queue 108, user discriminator 110 and user specific conditioner 112. User discriminator 110 can read a packet header to determine the appropriate user specific conditioner to which to send the packet based on for example, the IP address and MAC address of the packet. Bandwidth limits can be enforced based on user specific traffic control rules. According to one embodiment of the present invention, conditioning module 84 can locate the user specific traffic control rule based from user specific IP table 90. For example, for a packet having the originating MAC address 08:00:69:02:01:FF and the IP address 100.100.100, traffic conditioning module 84 can access user specific rule 92 and, from user

specific rule 92, user specific traffic control rule 94. The user specific traffic control rule can be enforced at the corresponding user specific conditioner.

Interface master queue 108 can control the flow of network traffic over a particular interface. It can be configured to send out data at whatever rate is appropriate for the corresponding network connection. Interface master queue 108 can be feed data by user specific conditioners 112, each of which can have its own queue to hold packets the conditioner has accepted, but interface master queue 108 is not ready to accept.

For a particular network interface, each user can have an inward (i.e., download) and outward (i.e., upload) bandwidth allowance, based on attributes in the user's user profile. A bandwidth limit is the maximum rate at which a user is permitted to transmit or receive network traffic over a particular interface. User specific traffic conditioners 112 ensure that, if a user exceeds his or her bandwidth allowance, further network traffic in that direction on the network will be queued or dropped until the average data rate fall back within the bandwidth allowance. Thus, traffic conditioning module 84 can regulate bandwidth on a per user basis. In one embodiment, the control device can also dynamically control bandwidth on a per user basis.

It should be noted that the architectures of FIGURE 4, FIGURE 5 and FIGURE 6 are provided by way of example only and authentication, session monitoring and provisioning can be implemented using any suitable programming language and/or structure known in the art. In the example of FIGURE 5, provisioning module 68 provides firewall and traffic conditioning based on a set of IP tables. It should be noted, however, that provisioning module 68 can provide additional services on a per user basis, such as virus scanning, worm detection or any other service known in the art. Each of these additional services can access rules and parameters based, for example, on IP table 90. Moreover, the use of IP tables to index and provide access to rules and parameters for particular services is also provided by way of example. In other embodiments of the present invention, a user profile can be mapped to rules and parameters for various applications in any suitable programming manner known in the art.

Embodiments of the present invention provide advantages over prior art systems and methods of providing access control. One advantage is that embodiments of the control device can detect network communications across a variety of protocols and direct a user to an

authentication interface. Another advantage provided by embodiments of the present invention is that provisioning can be done based on a user profile rather than based on a particular port. In other words provisioning of bandwidth and services can be done on a per user rather than per port basis. Additionally, as will be described in conjunction with FIGURE 7, embodiments of the present invention can provide advantages with respect to physical roaming.

FIGURE 7 is a diagrammatic representation of roaming according to one embodiment of the present invention. In the example of FIGURE 7, a LAN can have multiple subnets, in this case two, subnet 122 and subnet 124. For the sake of example, each subnet can be a wireless subnet. Each subnet could represent for example subnets on different floors of an office building or subnets in different buildings, etc. Each subnet can be connected to network 126 via control device 128 and control device 130, respectively. Network 126 can be any network known in the art including a LAN, the Internet, a wireless network a global communications network or any other network known in the art. According to one embodiment of the present invention, control device 128 and control device 130 can be in federation 132. This means that control device 128 and control device 132 have at least enough information about each other that they can send messages to each other over the LAN and/or over network 126 to exchange session information.

In operation, user 134 using user device 135 (e.g., a laptop or other computing device known in the art) can authenticate with control device 130 at point 136 in subnet 124. Because user 134 is in subnet 124 at point 136, user device 135 can be assigned a first IP address, for example 100.100.100. For the sake example, user device can also be associated with MAC address 08:00:69:02:01:FF. The user's active session can be indexed based on the first IP address, the MAC address and the user's credentials. User 134 can then roam outside of subnet 124, by for example, leaving the range of the wireless routers of subnet 124. Control device 130 can determine if user 134 is still active on subnet 124 by, for example, ARP pining and/or performing port scans on user device 135 at predetermined intervals.

If control device 130 can not locate user device on subnet 124, control device 130 can begin a time out timer. If the time out timer reaches a predetermined limit, control device 130 can close the control session, returning user 134 to his or her preauthenticated state. If, however, user 134 returns to subnet 124, as, for example, determined by the ARP pings and/or port

scans, within the time limit, control device 130 can reset the time out timer and keep the control session open. Assume, for the sake of example, that user 134 returns to point 138 in subnet 124 before the session is timed out, so his or her control session remains open. Thus, control device 130 can maintain user 134 in an authenticated state even though user 134 roamed outside of subnet 124.

User 134 can then roam from point 138 to point 140 with laptop 135. When user 134 leaves subnet 124, control device 130 can begin a time out timer for the user's control session. When user 134 enters subnet 122, laptop 135 can be assigned a new IP address for that subnet, say 101.100.100. If user 134 initiates a network communication destined for network 126 (e.g., a web page request), control device 128 can receive the communication and determine if IP address 101.100.100 and MAC address 08:00:69:02:01:FF correspond to an active control session. In this case, because user 134 authenticated with control device 130, IP address 101.100.100 and MAC address 08:00:69:02:01:FF will not correspond to an active session on control device 128. In one embodiment of the present invention, control device 128 can simply initiate a new authentication process.

In another embodiment of the present invention, control device 128 can query other control devices with which it is federated to determine if a user has an active control session. For example, because control device 128 and control device 130 are in federation 132, control device 128 can query control device 130 to determine if user 134 has an active session. This can be done based, for example, on the MAC address of laptop 135 as laptop 135 will typically retain the same MAC address across subnets.

According to one embodiment of the present invention, control device 128 can send an SNMP message to control device 130 to determine if there is an active session corresponding to the MAC address 08:00:69:02:01:FF. In this case, if the user's control session at control device 130 has not yet timed out, control device 130 can reply to control device 128 with session information and the user profile for user 134. Control device 128 can establish user based provisioning based on the user profile as if user 134 had authenticated at control device 128. Thus, user 134 can communicate to network 126 through control device 128 without reauthenticating.

In other embodiments of the present invention, active session information for each control device can be maintained at a centralized system. Control device 128 can, in this

embodiment of the present invention, query the centralized system as to whether there are any active session corresponding to MAC address 08:00:69:02:01:FF. In yet another embodiment of the present invention, control device 128 can receive the user profile for user 134 from an authentication system rather than from another control device.

Thus, embodiments of the present invention allow a user to physically roam, either in a wired or wireless environment, by, for example permitting mobile, transient behavior through the use of network access timeouts; and/or coordinating authentications between control devices.

As can be understood from the foregoing, physically moving from one location to another can cause a user device to become disconnected from the network or subnet (e.g., subnet 122 or subnet 124) for a short period of time. The length of the time the user is not connected can be a function of physically moving from one location to another. Embodiments of the present invention permit a configurable timeout period that allows an authenticated user to become disconnected from a network and then reappear without losing the user's authentication status. In one embodiment of the present invention, this timeout period can be part of the policy of the network service provider (e.g., the entity controlling subnet 122 and subnet 124) and, as such, is a configurable item in the control devices. The control devices can monitor user network device connection states actively, employing ARP ping techniques and non-obtrusive polling of network application ports to check the connection status of all authenticated users' devices.

A second aspect of physical roaming is when a user not only becomes disconnected from the network, but leaves a subnet arbitrated or monitored by a control device. In this case, once the user attempts any network access by way of a network access port (wired or wireless) at another control device, that control device can solicit feedback from any federation of control devices with which it has joined to determine if this particular user has an active session and should be granted a new session, without the requirement to authenticate. In some embodiments of the present invention, the new control device can dynamically remap the network connections and configuration of a roaming user's user device, in the event that the new control device is configured differently or controls a different subnet. For example, the new control device can remap the IP address of the user device according any IP mapping scheme known in the art.

Control devices can participate in federations, in one embodiment of the present invention, via loosely-coupled SNMP dialogs. In this embodiment of the present invention there is no permanent federation configuration and, instead, control devices can broadcast their authorization status requests dynamically.

Another aspect of roaming can be service roaming. Service roaming can be a function of negotiated usage agreements between internet service providers, resulting in cross-indexed user authentication database and, potentially, resulting surcharges for accessing network resources via service providers other than the primary service provider associated with a user; i.e., assuming network service is funded by an individual, there may be surcharges to access network services via control devices not owned by that service provider.

FIGURE 8 is a diagrammatic representation of one embodiment of a control device 141 that can provide access control and authentication. For the purposes of example, control device 141 can comprise a main bus 142, a main processor 144, a primary storage medium 146, a secondary storage controller 148, a storage media 150, a user side network interface 152 and a controlled network network interface 154. The network interfaces can include Ethernet interfaces, fibre channel interfaces, T1 interfaces, wireless interfaces or other network interfaces known in the art. Other devices may be connected to or be part of such a control device include, by way of example, but not limitation, controllers, a display, a mouse, a keyboard, and so forth. Additionally, control device 140 can include additional interfaces to communicate to additional networks using various protocols and can include interfaces for administrative functions.

The main processor 144 communicates with the other components by way of the main bus 142. This main processor 144 can be a general purpose processor, a limited processor such as an ASIC or microcontroller, or any other instruction execution machine. The primary storage 146 can provide transient memory or storage space for use by programs executing on the main processor 144. The main processor 144 communicates with the primary storage in any manner known in the art.

The secondary storage controller 148 connects a storage media 150 such as a hard drive, CD-ROM, floppy, tape drive, optical storage medium, memory or other storage device to the main processor 144 by way of the main bus 142. The main processor 144 communicates with the secondary storage controller 148 by way of the main bus 142, and the secondary storage

controller 148 is used to read and /or write the storage media 150 on behalf of the main processor 144.

Control device 141 may communicate with other computing devices (e.g., user devices, network servers, etc.) by way of networks using network interfaces (e.g., user side network interface 152 and controlled network network interface 154 or other network interface). Computer instructions running on the main processor may then access other computers across the network in any of the conventional ways, e.g. by executing "protocols" which affect the transmission and reception of protocol data units, packages, etc. over the data transmission network.

In one embodiment of the present invention, storage media 150 can store a set of computer instructions 156 that are executable by processor 144. During execution, portions of computer instructions 156 and data can be stored in primary storage 146, as would be understood by those of ordinary skill in the art. Processor 144 can execute computer instructions 156 to authenticate users and/or provide provisioning to users on a per user basis. Computer instructions 156 may be implemented in any programming language known in the art and can be implemented using any suitable architecture.

Additionally, in one embodiment of the present invention, storage media 150 can include a database of user profiles an authentication credentials. In this embodiment of the present invention, instructions 156 can be executable to authenticate the user at control device 141 and receive the user profile from storage media 150.

Although shown as a standalone device in FIGURE 8, control device 141 may be integrated with and share components with other devices such as routers, servers, hubs or other devices known in the art. Additionally, computer instructions 156 can be distributed across multiple storage media and can be executed by multiple processors. One example of an exemplary control device is the Rock Box or the Rocksteady NSA Server, from Rocksteady Networks, Inc. of Austin, Texas.

While the present invention has been described with reference to particular embodiments, it should be understood that the embodiments are illustrative and that the scope of the invention is not limited to these embodiments. Many variations, modifications, additions and improvements to the embodiments described above are possible. It is contemplated that these

variations, modifications, additions and improvements fall within the scope of the invention as detailed in the following claims.

5

CLAIMS

1. A system of providing network access comprising:

a processor;

a first network interface coupled to the processor;

a second network interface coupled to the processor;

a storage media accessible by the processor;

a set of computer instructions stored on the storage media, executable by the processor to:

receive a network communication over the first network interface from a user device associated with a user;

determine if the network communication is associated with an authenticated user;

if the network communication is not associated with an authenticated user, direct the user to an authentication interface;

receive credentials from the user;

authenticate the user based on the credentials,

receive a user profile if the user is authenticated.

2. The system of Claim 1, wherein the computer instructions are further operable to monitor a network connected to the first network interface for the network communication.

3. The system of Claim 2, wherein the computer instructions are further operable to monitor the network across multiple protocols.

4. The system of Claim 1, wherein the network communication comprises an HTTP request and wherein the computer instructions are further executable to:

receive the HTTP request;

send a redirect request to the user device to redirect a web browser to the authentication interface.

5. The system of Claim 1, wherein the network communication comprises an email and wherein the computer instructions are further executable to:

receive the email;

determine a protocol for the email;

send a reply email message to the user device directing the user to the authentication interface.

6. The system of Claim 1, wherein the computer instructions are further executable to:

determine a network protocol for the network communication;

send a reply to the user device according to the network protocol directing the user to the authentication interface.

7. The system of Claim 6, wherein the network protocol is one of HTTP, SMTP, POP, telnet, UDP or FTP.

8. The system of Claim 1, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by comparing an identifier associated with the network communication to identifiers associated with authenticated users.

9. The system of Claim 8, wherein the identifier comprises an IP address for the user device.

10. The system of Claim 8, wherein the identifier comprises a MAC address for the user device.

11. The system of Claim 1, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by contacting a federated device.

12. The system of Claim 1, wherein the computer instructions are further executable to receive the user profile from an internal source.

13. The system of Claim 1, wherein the computer instructions are further executable to:

transmit the credentials to an authentication system; and

receive the user profile from the authentication system if the user is authenticated.

14. The system of Claim 1, wherein the computer instructions are further executable to:

provision the user with access to a network connected to the second network interface based on the user profile.

15. The system of Claim 14, wherein the computer instructions are further executable to provision the user with access to the network by provisioning user specific bandwidth based on the user profile.

16. The system of Claim 15, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

17. The system of Claim 16, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

18. The system of Claim 17, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

19. The system of Claim 18, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

20. The system of Claim 14 wherein the computer instructions are further executable to provision the user with access to the network by establishing user specific firewall rules and enforcing the user specific firewall rules.

21. The system of Claim 1, wherein the computer instructions are executable to monitor a control session for the user to determine if the user times out.

22. The system of Claim 21, wherein the computer instructions are further executable to close the control session if the user times out.

23. A system of providing network access comprising:

a processor;

a first network interface coupled to the processor;

a second network interface coupled to the processor;

a storage media accessible by the processor;

a set of computer instructions stored on the storage media, executable by the processor to:

receive a user profile; and

provision a user on a first network connected to the first network interface with access to a second network connected to the second network interface based on the user profile.

24. The system of Claim 23, wherein the computer instructions are further executable to provision the user with access to the second network by provisioning user specific bandwidth to the user based on the user profile.

25. The system of Claim 24, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

26. The system of Claim 25, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

27. The system of Claim 26, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

28. The system of Claim 27, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

29. The system of Claim 23 wherein the computer instructions are further executable to provision the user with access to the second network by establishing user specific firewall rules and enforcing the user specific firewall rules.

30. The system of Claim 23, wherein the user profile comprises one or more attributes that govern the provisioning of user's access to the second network.

31. The system of Claim 23, wherein the computer instructions are further executable to authenticate the user.

32. A system of providing network access comprising

a set of computer instructions stored on a storage media, executable by a processor to:

receive a network communication over a first network interface from a user device associated with a user;

determine if the network communication is associated with an authenticated user;

if the network communication is not associated with an authenticated user, direct the user to an authentication interface;

receive credentials from the user;

authenticate the user based on the credentials,

receive a user profile if the user is authenticated.

33. The system of Claim 32, wherein the computer instructions are further operable to monitor a network for the network communication.

34. The system of Claim 33, wherein the computer instructions are further operable to monitor the network across multiple protocols.

35. The system of Claim 32, wherein the network communication comprises an HTTP request and wherein the computer instructions are further executable to:

receive the HTTP request;

send a redirect request to the user device to redirect a web browser to the authentication interface.

36. The system of Claim 32, wherein the network communication comprises an email and wherein the computer instructions are further executable to:

receive the email;

determine a protocol for the email;

send a reply email message to the user device directing the user to the authentication interface.

37. The system of Claim 32, wherein the computer instructions are further executable to:

determine a network protocol for the network communication;

send a reply to the user device according to the network protocol directing the user to the authentication interface.

38. The system of Claim 37, wherein the network protocol is one of HTTP, SMTP, POP, telnet, UDP or FTP.

39. The system of Claim 32, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by comparing an identifier associated with the network communication to identifiers associated with authenticated users.

40. The system of Claim 39, wherein the identifier comprises an IP address for the user device.

41. The system of Claim 39, wherein the identifier comprises a MAC address for the user device.

42. The system of Claim 32, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by contacting a federated device.

43. The system of Claim 32, wherein the computer instructions are further executable to receive the user profile from an internal source.

44. The system of Claim 32, wherein the computer instructions are further executable to:

transmit the credentials to an authentication system; and

receive the user profile from the authentication system if the user is authenticated.

45. The system of Claim 32, wherein the computer instructions are further executable to:

provision the user with access to a network based on the user profile.

46. The system of Claim 45, wherein the computer instructions are further executable to provision the user with access to the network by provisioning user specific bandwidth based on the user profile.

47. The system of Claim 46, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

48. The system of Claim 47, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

49. The system of Claim 48, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

50. The system of Claim 49, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

51. The system of Claim 45 wherein the computer instructions are further executable to provision the user with access to the network by establishing user specific firewall rules and enforcing the user specific firewall rules.

52. The system of Claim 32, wherein the computer instructions are executable to monitor a control session for the user to determine if the user times out.

53. The system of Claim 52, wherein the computer instructions are further executable to close the control session if the user times out.

54. A system of providing network access comprising:

a set of computer instructions stored on the storage media, executable by the processor to:

receive a user profile;

provision a user with access to a network based on the user profile.

55. The system of Claim 54, wherein the computer instructions are further executable to provision the user with access to the network by provisioning user specific bandwidth based on the user profile.

56. The system of Claim 55, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

57. The system of Claim 56, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

58. The system of Claim 57, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

59. The system of Claim 58, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

60. The system of Claim 54 wherein the computer instructions are further executable to provision the user with access to the network by establishing user specific firewall rules and enforcing the user specific firewall rules.

61. The system of Claim 54, wherein the user profile comprises one or more attributes that govern the provisioning of user's access to the network.

62. The system of Claim 54, wherein the computer instructions are further executable to authenticate the user.

63. A method of providing network access comprising

receiving a network communication over a first network interface from a user using a user device;

determining if the network communication is associated with an authenticated user;

if the network communication is not associated with an authenticated user, directing the user to an authentication interface;

receiving credentials from the user;

authenticating the user based on the credentials,

receiving a user profile if the user is authenticated.

64. The method of Claim 63, further comprising:
determining a network protocol for the network communication;
sending a reply to the user device according to the network protocol directing the user to the authentication interface.

65. The method of Claim 64, wherein the network protocol is one of HTTP, SMTP, POP, telnet, UDP or FTP.

66. The method of Claim 63, further comprising determining if a network communication is associated with an authenticated user by comparing an identifier associated with the network communication to identifiers associated with authenticated users.

67. The method of Claim 63, further comprising determining if a network communication is associated with an authenticated user by contacting a federated control device.

68. The method of Claim 63, further comprising:
transmitting the credentials to an authentication system;
receiving the user profile from the authentication system.

69. A method of providing network access comprising:
receiving a user profile;
provisioning a user with access to a network based on the user profile.

70. The method of Claim 69, further comprising establishing a traffic control rule based on the user profile.

71. The method of Claim 70, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

72. The method of Claim 70, further comprising:

receiving a packet;

determining that the traffic control rule applies to the packet based on an identifier extracted from the packet;

applying the traffic control rule to the packet.

73. The method of Claim 72, further comprising dropping the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

74. The method of Claim 69, further comprising establishing user specific firewall rules based on the user profile and enforcing the user specific firewall rules.

75. The method of Claim 69, wherein the user profile comprises one or more attributes that govern the provisioning of user's access to the network.

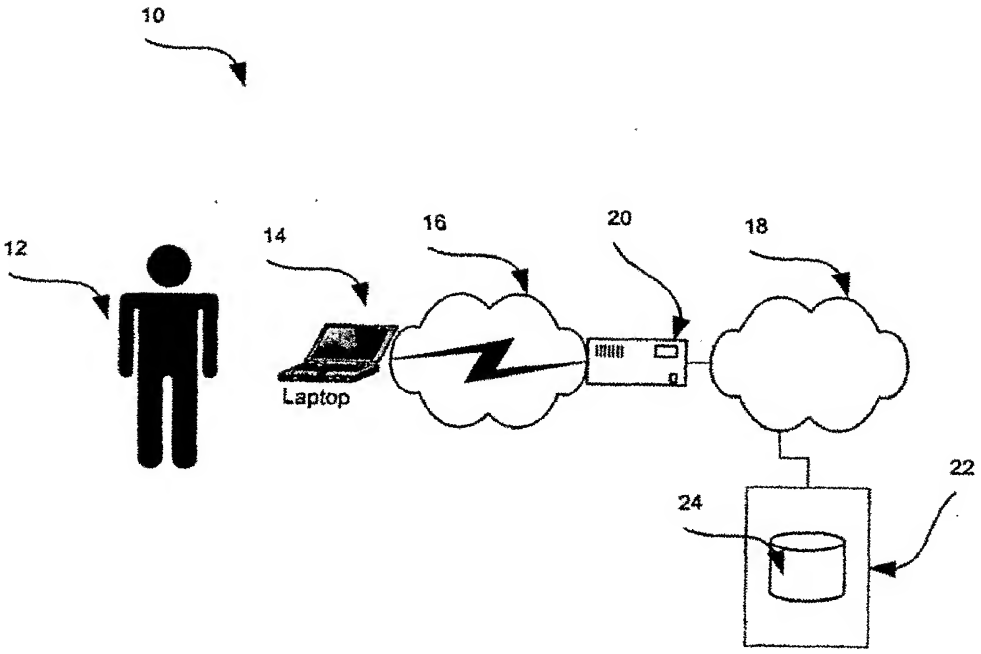


FIG. 1

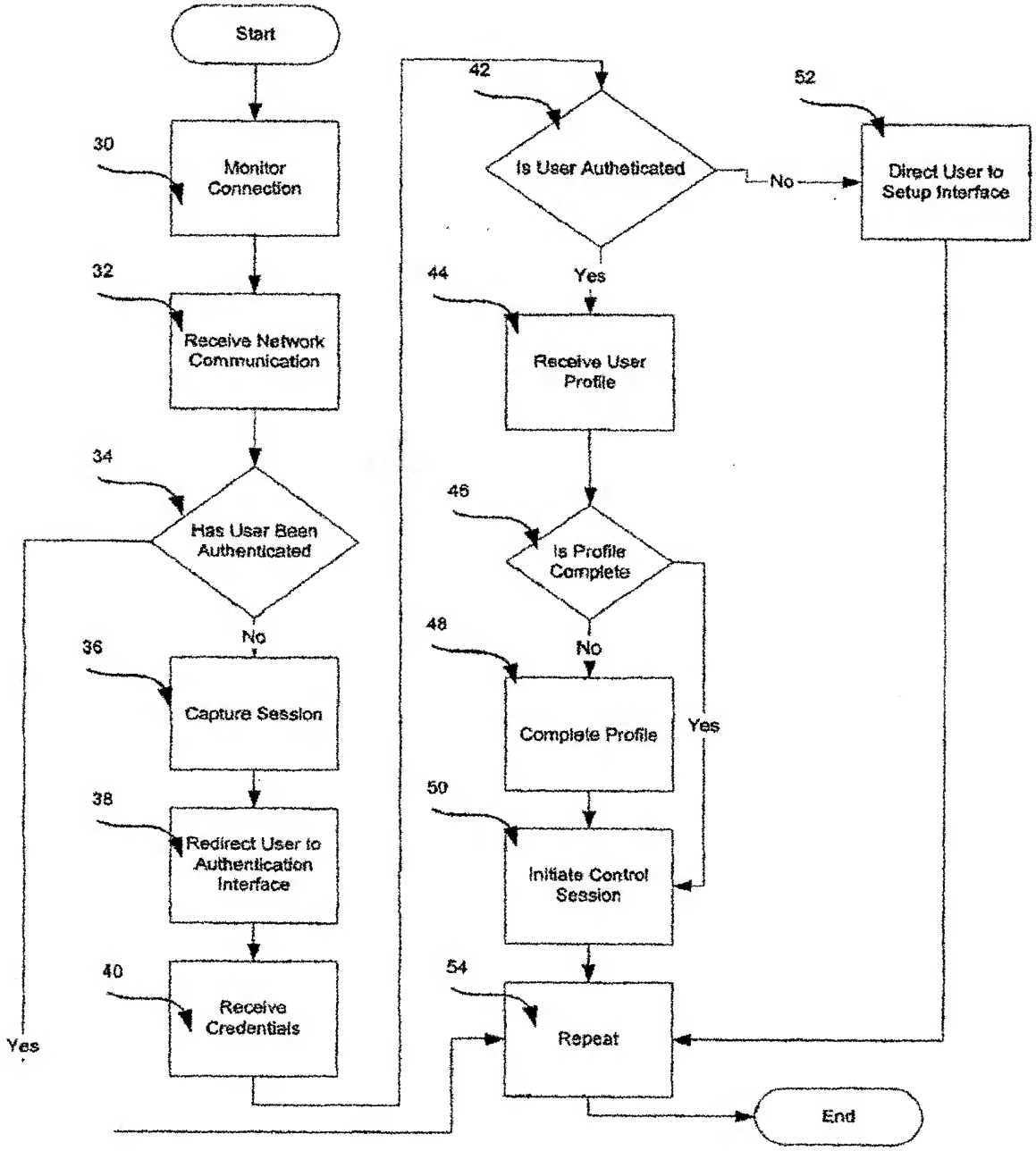

Start
30
Monitor Connection
32
Receive Network Communication
34
Has User Been Authenticated
No
Yes
36
Capture Session
38
Redirect User to Authentication Interface
40
Receive Credentials
42
Is User Autheticated
No
52
Direct User to Setup Interface
Yes
44
Receive User Profile
46
Is Profile Complete
No
Yes
48
Complete Profile
50
Initiate Control Session
54
Repeat
End

FIGURE 2

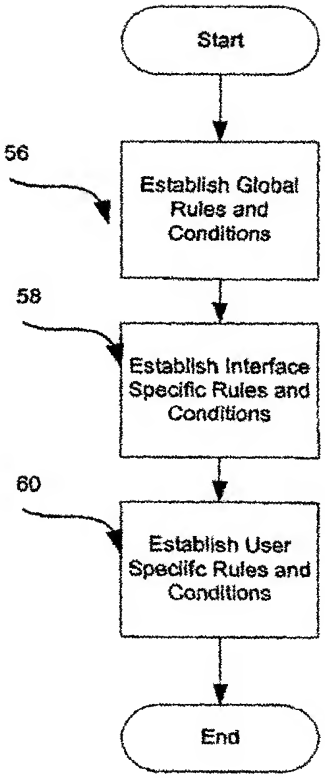

Start
56
Establish Global Rules and Conditions
58
Establish Interface Specific Rules and Conditions
60
Establish User Specific Rules and Conditions
End

FIGURE 3

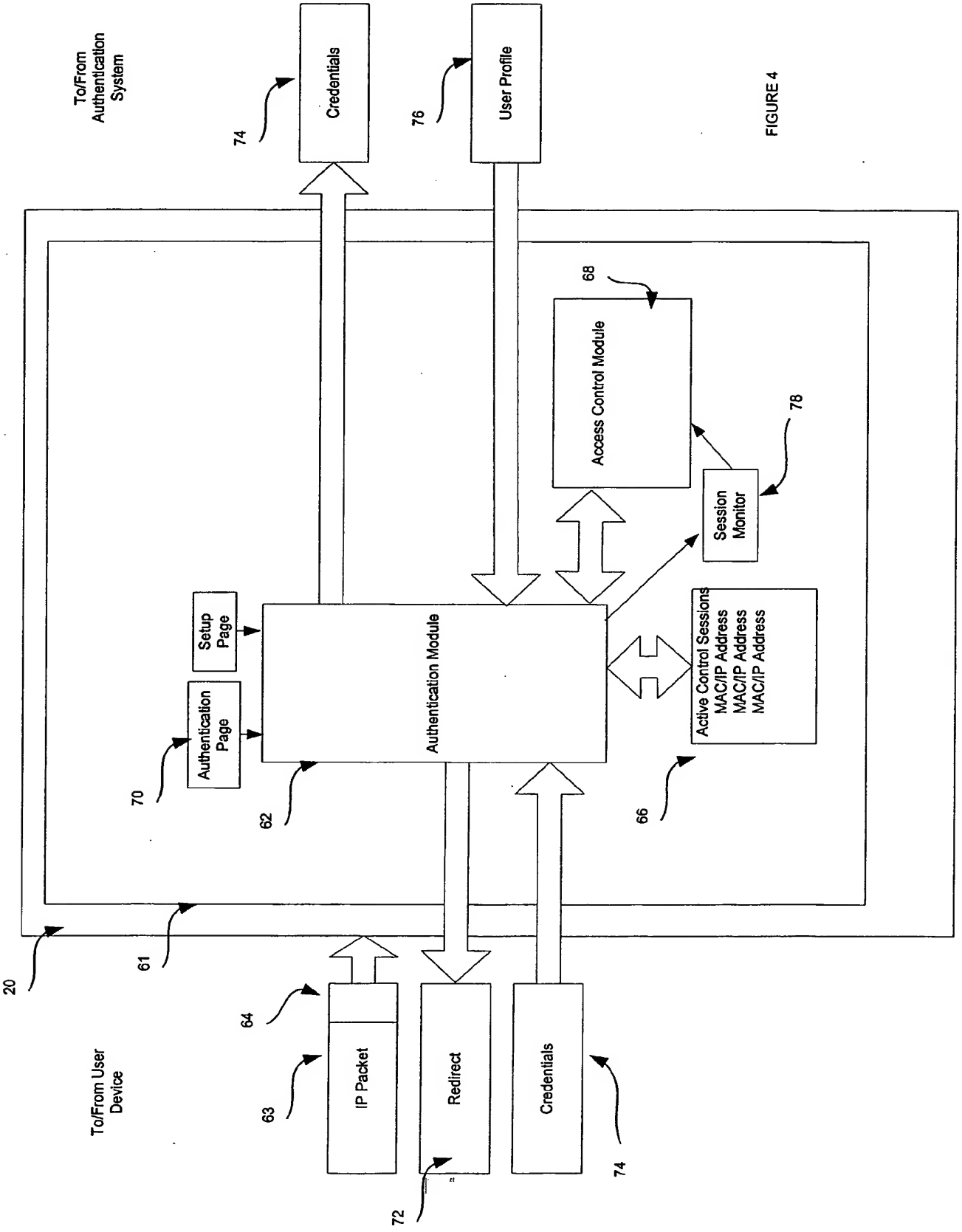

To/From Authentication System
Credentials
User Profile
74
76
68
Access Control Module
78
Session Monitor
Setup Page
Authentication Page
Authentication Module
Active Control Sessions
MAC/IP Address
MAC/IP Address
MAC/IP Address
70
62
66
20
61
64
63
IP Packet
Redirect
Credentials
72
74
To/From User Device

FIGURE 4

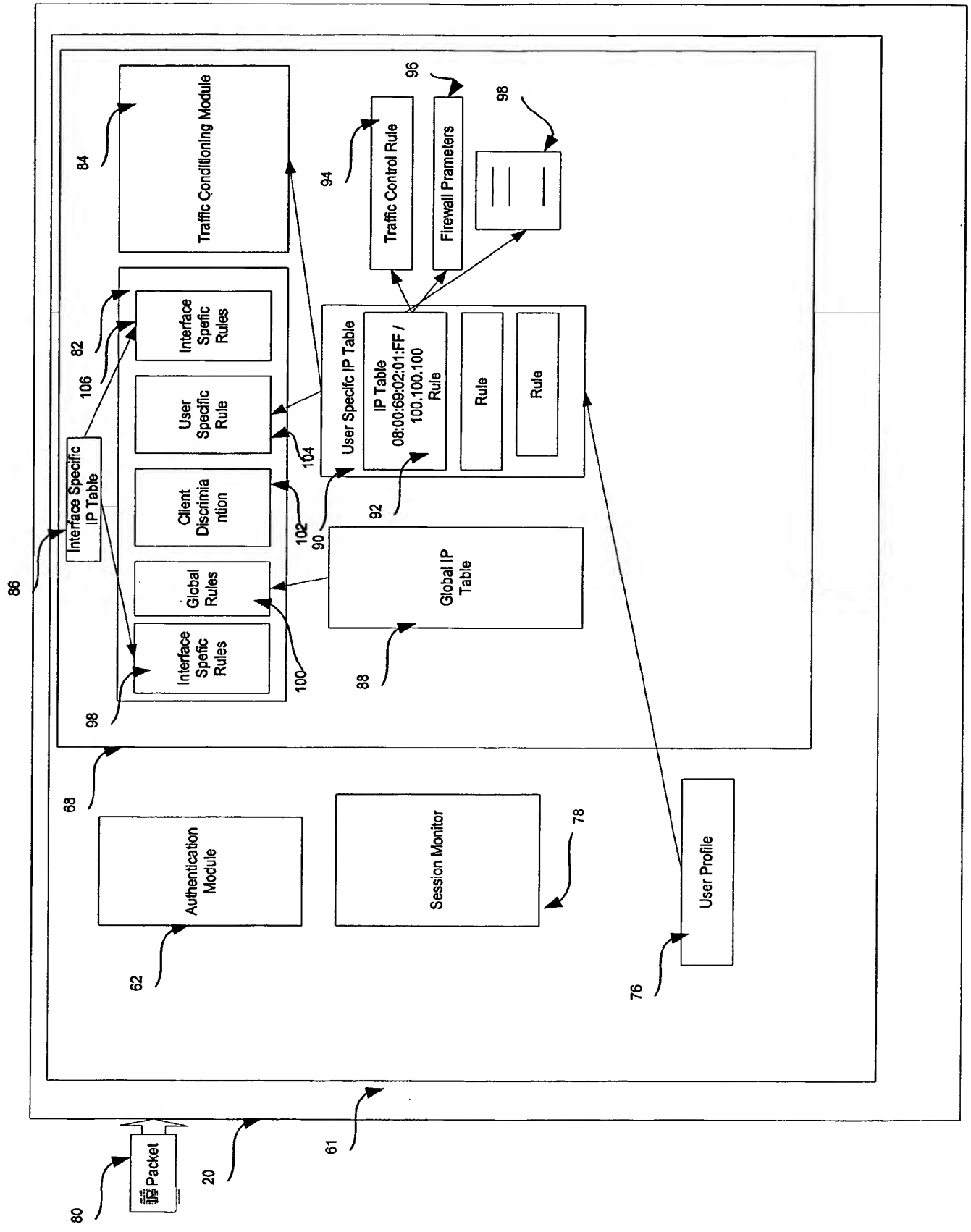

Packet
80
20
61
86
Traffic Conditioning Module
84
Traffic Control Rule
94
96
Firewall Prameters
98
Interface Specific IP Table
106
82
Interface Spefic Rules
User Specific Rule
104
Client Discrimination
Global Rules
Interface Spefic Rules
98
100
102
90
User Specifc IP Table
IP Table 08:00:69:02:01:FF / 100.100.100 Rule
Rule
Rule
92
Global IP Table
88
68
Authentication Module
62
Session Monitor
78
User Profile
76

FIGURE 5

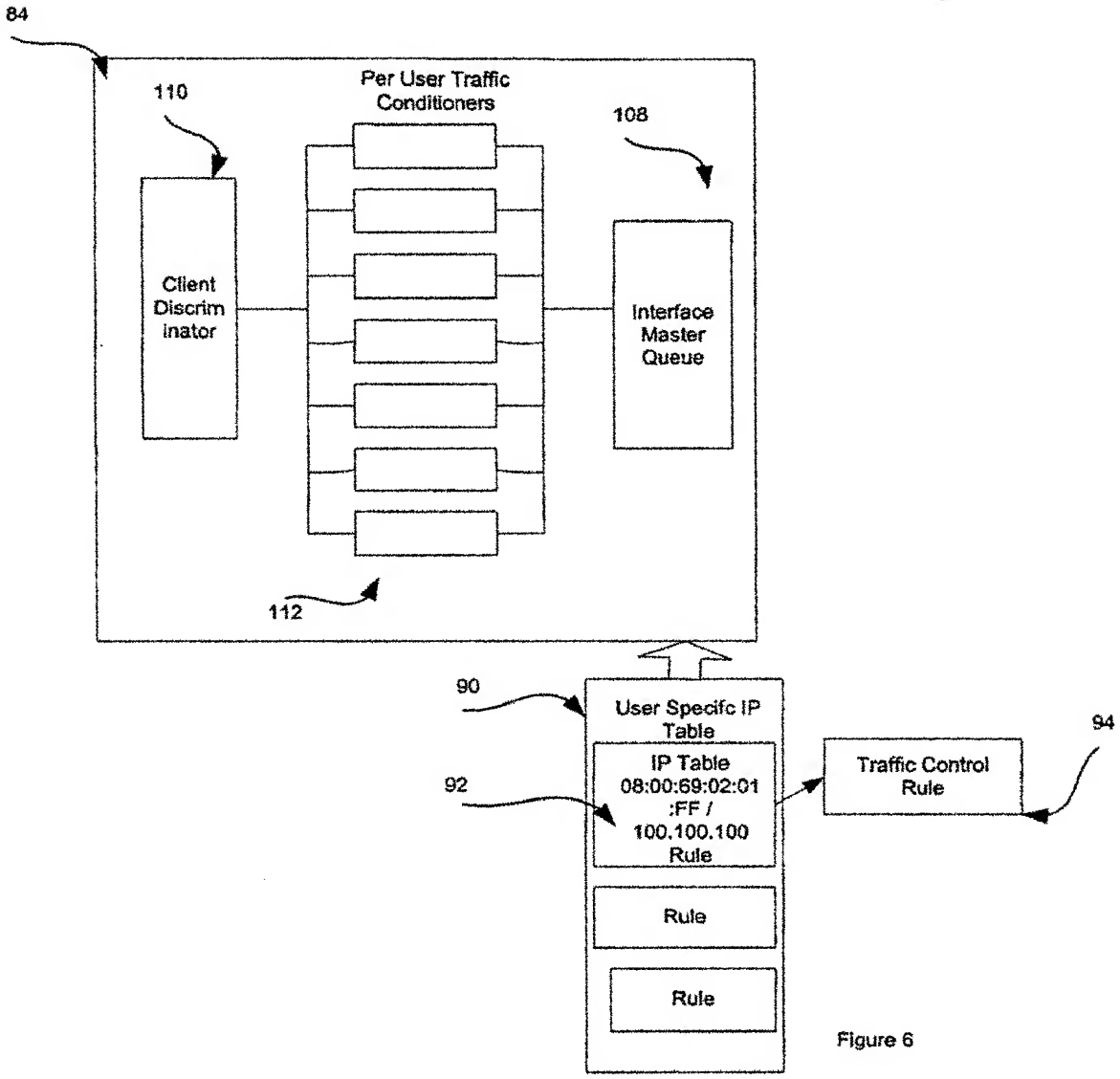

84
110
Per User Traffic Conditioners
108
Client Discrim inator
Interface Master Queue
112
90
User Specifc IP Table
IP Table 08:00:69:02:01 :FF / 100.100.100 Rule
92
Traffic Control Rule
94
Rule
Rule

Figure 6

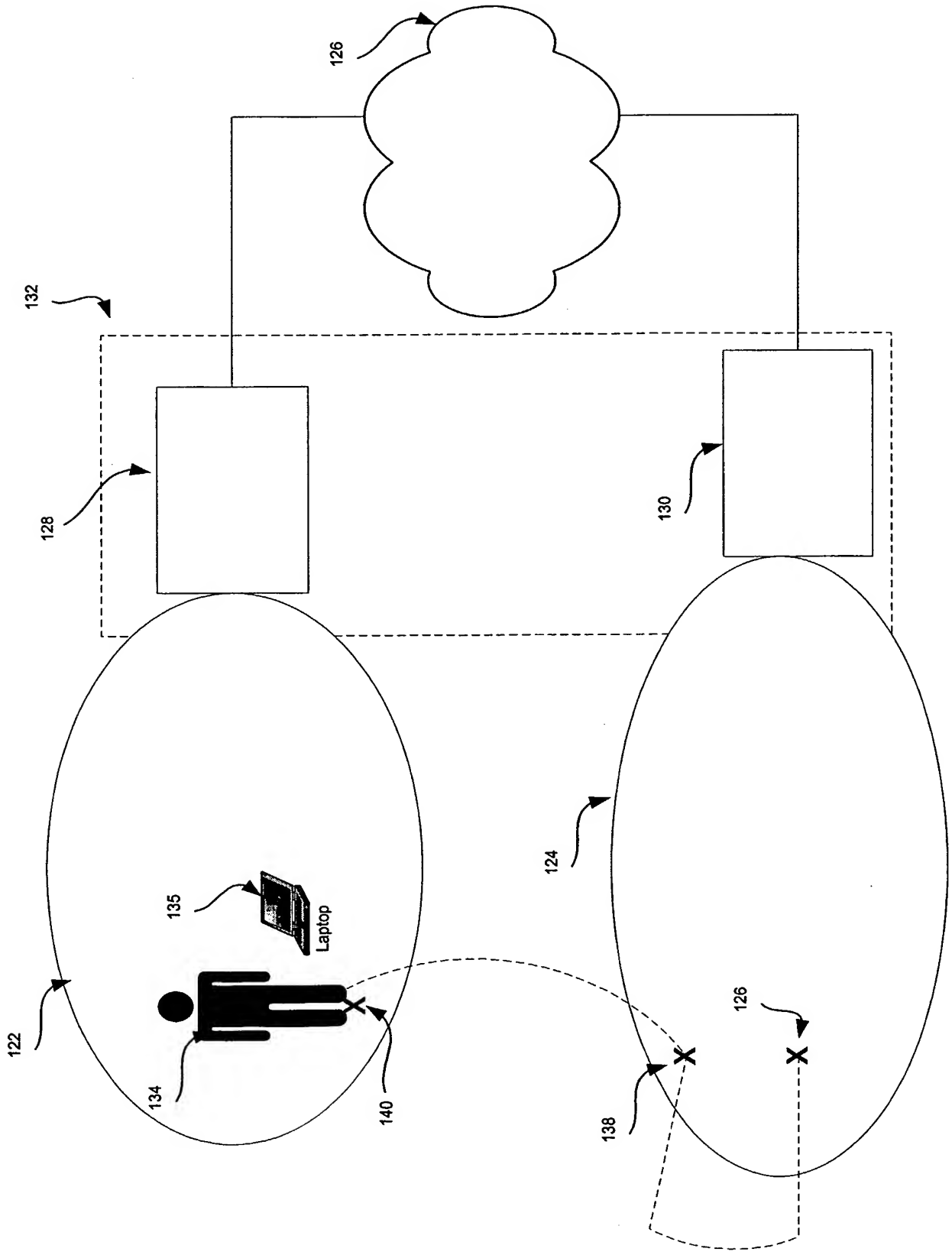
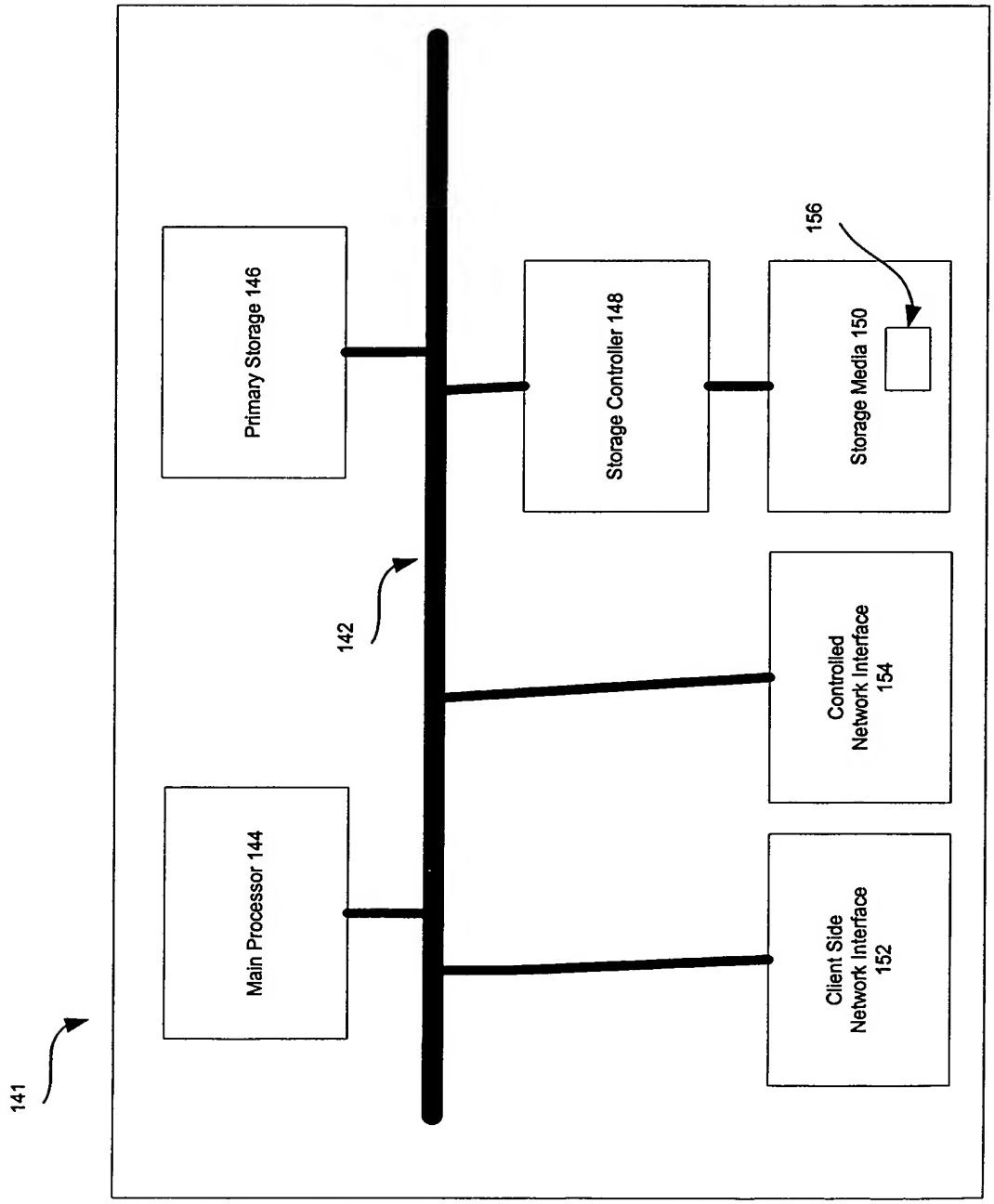

126
132
128
130
124
135
Laptop
122
134
140
138
126

FIGURE 8


141
142
Main Processor 144
Primary Storage 146
Client Side Network Interface 152
Controlled Network Interface 154
Storage Controller 148
Storage Media 150
156